

RECEIVED
CENTRAL FAX CENTER
AUG 22 2007

REMARKS

The above-identified application is United States application serial number 10/749,200 filed on December 31, 2003. Claims 1-31 are pending in the application. Claims 1-31 are rejected.

Claim Rejections under 35 U.S.C. §112

Claims 8, 16 and 24 rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicants believe "scanning" is an appropriate description of the sequential receipt of data, as described, but have amended the claims to replace "scanning" with "receiving in sequence" to possibly more correctly describe the operation.

Rejection of Claims under 35 U.S.C. §103

Claims 1-3, 7 and 9 are rejected under 35 U.S.C. §103(a) as being unpatentable over Coppersmith. Applicants have amended the claims to clarify that input connections are made to the claimed structures rather than a capability of such connection, thereby further distinguishing over Coppersmith. The Examiner admits that Coppersmith does not teach that the first input block is a text block contains a secret PIN, does not teach that the second input block is derived from a non-secret entity-identifier, and does not teach that the key is a Pin Verification Key. The Coppersmith disclosure neither describes nor even hints that input connections including the secret PIN and non-secret identity identifier can be used to improve PIN verification.

KSR International Co. v. Teleflex, Inc., et al., 550 U.S. ___, 127 S.Ct. 1727 (2007) requires that an Examiner must provide "some articulated reasoning with some rationale underpinning to support the legal conclusion of obviousness" (KSR opinion, page 14), and must "identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed Invention does" (KSR opinion, page 15). In the present case, the Examiner fails to identify reasons for connecting the secret PIN to the first input block and for

COESTNER BERTANI LLP
2192 MARTIN ST.
SUITE 150
IRVINE, CA 92613
TEL (949) 251-0250
FAX (949) 251-0260

connecting the non-secret identity identifier to the second input block other than that such connection could be made. Accordingly, the Examiner uses impermissible hindsight to modify the reference into the claimed form. In light of the omissions in the cited references, according to KSR, the Examiner must make "explicit" the rationale of the "apparent reason to combine the references in the fashion claimed" (KSR opinion, page 14).

Applicants have amended Claim 3 to clarify that the apparatus operates in a reversible mode that actively recovers the secret PIN from the second ciphertext block, rather than claiming merely such a capability. Claim 3 further distinguishes over Coppersmith which neither describes nor hints of recovery of the secret PIN as claimed or operation in the reversible mode.

Claims 4-5 are rejected under 35 U.S.C. §103(a) as being unpatentable over Coppersmith in view of Vernam (1310719). Applicants traverse the rejections. The Examiner admits that Coppersmith does not teach a logical operator that exclusive-ORs the first ciphertext block with the second ciphertext block to produce a third ciphertext block, but states that Vernam teaches a cipher that takes in two inputs and XORs them together to produce a ciphertext. However Vernam does not teach first and second ciphertexts that are combined to produce a ciphertext, but rather discloses combination of a plaintext block with a ciphertext block. Accordingly, the combination of Coppersmith and Vernam does not operate as claimed by the applicants. Regarding Claim 5, the combination of Coppersmith and Vernam neither describes nor hints of recovery of the secret PIN from the second ciphertext block as claimed or operation in the irreversible mode as claimed.

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith in view of Vernam as applied to claim 5 above, and further in view of Briachtl. Claim 6 is patentable at least on the basis of depending from an allowable base claim.

Claims 8 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith in view of Matyas. Applicants have amended Claim 8 to clarify that the format converter converts hexadecimal ciphertext to decimal. Claim 8 is patentable at least on the basis of depending from an allowable base claim but is

KOESTNER BERTANI LLP
2192 MARTIN ST.
SUITE 150
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260

further patentable because Coppersmith in view of Matyas do not disclose the format converter coupled to a cipher block in the CBC chain or generation of output digits as a PIN verification value, as claimed. The Examiner cites the lapse of time since discovery of pin verification (the late 1970's for IBM 3624) as motivation for making the combination. Applicants view such a lapse of time as irrelevant to motivation or actually evidence against motivation since no such combination has been made since that time.

Regarding Claim 10, the Examiner admits that Coppersmith does not teach the first and second plaintext blocks as claimed but uses Matyas to justify such a format. The applicants traverse the rejection on the basis that Matyas does not disclose the plaintext block formats as claimed but merely gives definitions of the entities claimed by the applicants. Such definitions are not disputed to be known. What is novel and nonobvious is the connection of the plaintext blocks, as claimed, to improve PIN verification.

Claims 11-13, 16-21 and 24-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas in view of Coppersmith. Applicants traverse the rejections. The Examiner admits Matyas does not teach a method of linking a plurality of cipher blocks, applying incoming plaintext blocks to cipher blocks, keying the cipher blocks with a key, XORing the plaintext block with an initialization vector, encrypting the initialized block using tripled DES encryption, XORing the plaintext block with the first ciphertext block, encrypting the chained block using triple DES encryption, and outputting the second cipher block. The Examiner uses Coppersmith to support elements that are missing from Matyas, however even combining Coppersmith with Matyas fails to disclose applying an incoming plaintext block derived fro a secret PIN to a cipher block, applying an incoming plaintext block derived from a non-secret entity-identifier and ciphertext from a cipher block in the CBC chain, and keying the cipher blocks with a secret PVK.

In stating "[i]t would have been obvious to one of ordinary skill in the art at the time of the invention to have the processor of Matyas perform the method of Coppersmith" with the motivation that "using a CBC using triple-DES encryption is well known in the art," the Examiner has given absolutely no reasoning for making

KOESTNER BERTANI LLP
2192 MARTIN ST
SUITE 150
IRVINE, CA 92612
TEL (714) 251-0230
FAX (714) 251-0260

the combination of references, but merely makes an unsupported conclusion. *KSR International Co. v. Teleflex, Inc., et al.*, 550 U.S. ___, 127 S.Ct. 1727 (2007) requires that an Examiner must provide "some articulated reasoning with some rationale underpinning to support the legal conclusion of obviousness" (KSR opinion, page 14), and must "identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed invention does" (KSR opinion, page 15).

The Examiner further admits that Coppersmith does not teach that the first input block that is a text block contains a secret PIN, does not teach that the second input block is derived from a non-secret entity-identifier, does not teach that the key is a Pin Verification Key, and does not teach that the output of the second ciphertext block is to be used for the purpose of PIN verification. Applicants dispute the obviousness of having the system of Coppersmith input a secret PIN in the first input block and input a non-secret identifier in the second input block and have the key be a PIN verification key since Matyas does not disclose application of a secret PIN and a non-secret identifier to a PIN verification system. The Examiner gives motivation for the combination that "Coppersmith without any modification can take the inputs of a secret PIN and the non-secret identifier and using a key output a Pin Verification Value." However, Matyas does not disclose application of the secret PIN and non-secret identifier to a PIN verification apparatus.

Regarding Claims 16 and 24, the claims are patentable at least on the basis of depending from an allowable base claim and are further patentable because Matyas in view of Coppersmith do not disclose the format converter coupled to a cipher block in the CBC chain or generation of output digits as a PIN verification value, as claimed. The Examiner cites the lapse of time since discovery of pin verification (the late 1970's for IBM 3624) as motivation for making the combination. Applicants view such a lapse of time as irrelevant to motivation or actually evidence against motivation since no such combination has been made since that time.

Regarding Claims 17 and 25, the claims are patentable at least on the basis of depending from an allowable base claim.

KOESTNER BERTANI LLP
3193 MARTIN ST.
SUITE 150
IRVINE, CA 92610
TEL (949) 351-0250
FAX (949) 351-0260

Regarding Claims 19 and 27, the claims are patentable at least on the basis of depending from an allowable base claim and are further patentable because Matyas in view of Coppersmith do not disclose first and second plaintext blocks in the format as claimed. The applicants traverse the rejection on the basis that Matyas does not disclose the plaintext block formats as claimed but merely gives definitions of the entities claimed by the applicants. Such definitions are not disputed to be known. What is novel and nonobvious is the connection of the plaintext blocks, as claimed, to improve PIN verification.

Claims 14 and 22 are rejected under 35 U.S.C. §103(a) as being unpatentable over Matyas in view of Coppersmith as applied to claims 11 and 20 above, and further in view of Vernam. Applicants traverse the rejections. Claims 14 and 22 are patentable at least on the basis of depending from an allowable base claim and are further patentable because Vernam does not teach first and second ciphertexts that are combined to produce a ciphertext, but rather discloses combination of a plaintext block with a ciphertext block. Accordingly, the combination of Matyas, Coppersmith, and Vernam does not operate as claimed by the applicants.

Claims 15 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas in view of Coppersmith further in view of Vernam as applied to claims 14 and 22 above, and further in view of Brachtl. Claims 15 and 23 are allowable at least on the basis of depending from allowable base claims.

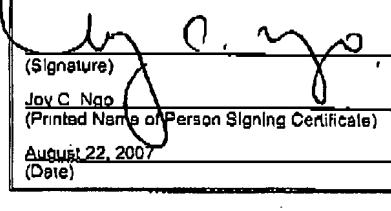
KOESTNER BERTANI LLP
3192 MARTIN ST.
SUITE 130
IRVINE, CA 92613
TEL (714) 251-0250
FAX (714) 251-0260

RECEIVED
CENTRAL FAX CENTER
AUG 22 2007

CONCLUSION

The application, including all remaining Claims 1-31, is believed to be in condition for allowance and a notice to that effect is solicited. Nonetheless, should any issues remain that might be subject to resolution through a telephonic interview, the examiner is requested to telephone the undersigned at (949) 251-0250.

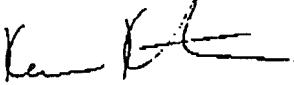
I hereby certify that this correspondence is being facsimile transmitted to the USPTO. Central Number at (571) 273-6300 on the date shown below:


(Signature)

Joy C. Ngo
(Printed Name or Person Signing Certificate)

August 22, 2007
(Date)

Respectfully submitted,



Ken J. Koestner
Attorney for Applicant(s)
Reg. No. 33,004

KOESTNER BERTANI LLP
2191 MARTIN ST.
SUITE 150
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0260